



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

09/932,882

08/20/2001

Martin J. Koistinen

09469.007001

6775

22511

7590

07/24/2006

OSHA LIANG L.L.P.  
1221 MCKINNEY STREET  
SUITE 2800  
HOUSTON, TX 77010

EXAMINER

SCHUBERT, KEVIN R

ART UNIT

PAPER NUMBER

2137

DATE MAILED: 07/24/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/932,882

Applicant(s)

KOISTINEN ET AL.

Examiner

Kevin Schubert

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 29 June 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-8, 10-16, 18-23 and 25-37 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-5, 7, 8, 10-16, 18-20, 22, 23 and 25-37 is/are rejected.
- 7) ☒ Claim(s) 6 and 21 is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |   |   |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)  | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date <u>12082003</u> | 6) <input type="checkbox"/> Other: _____  |

Art Unit: 2137

**DETAILED ACTION**

Claims 1-8,10-16,18-23, and 25-37 have been considered. Examiner thanks Applicant for his careful review of the previous action. Upon review, Examiner allows claims 6 and 21 and rejects all other pending claims based on a new ground(s) of rejection necessitated by Applicant's amendment.

5

***Allowable Subject Matter***

Claims 6 and 21 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims. More specifically, in the instant Remarks Applicant argues that the limitation "wherein the security device is a smartcard" is not rendered obvious over Gien, U.S. Patent Application Publication No. 2002/0112156, because the Gien reference "teaches away" from the combination (Remarks: page 7 final paragraph). Examiner agrees.

Because the Gien reference teaches that only the entity that issues the smart card can unblock it for security reasons, Gien teaches away from a system in which a client-side transfer agent performs the unblocking of a smart card by receiving an unblock code from an unblocking service. A search in the prior art reveals no reference which embodies a client-side transfer agent performing unblocking of a **smart card** by receiving an unblock code from an unblocking service, let alone one consistent with the foregoing and an obvious combination with the Lipsit, Takae, Chmaytelli, and Friedman references.

20

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

25

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

30

Art Unit: 2137

Claims 1-2,5,7,11-13,18-20,26,29-32, and 36-37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lipsit, EP 0820207 A2, in view of Takae, U.S. Patent Application Publication No. 2002/0034940, in further view of Chmaytelli, U.S. Patent No. 6,542,729, in further view of Friedman, U.S. Patent No. 6,240,513.

5

As per claims 1 and 18, the applicant describes an apparatus to unblock a security device issued to an end user comprising the following limitations which are met by Lipsit in view of Takae in further view of Chmaytelli in further view of Friedman:

- a) a client-side transfer agent for securely transferring information among the unblocking service,  
10 the end user, and the security device (Lipsit: page 5, line 47 to page 6, line 17);
- b) an agent-side transfer agent for securely transferring information between the unblocking service and a security agent (Lipsit: page 5, line 47 to page 6, line 17);
- c) an Unblock Authorization Code (UAC) generated after verification by the security agent and  
15 securely transferred from the agent-side transfer agent to the unblocking service, wherein verification comprises verifying the end user is assigned the security device while the end user is in possession of the security device (Lipsit: page 5, lines 47-50; Takae: [0084]);
- d) an Unblock Code (UBC) securely transferred from the unblocking service to the client-side transfer agent, wherein the client-side transfer agent uses the UBC to unblock the security device,  
(Chmaytelli: Col 8, lines 59-66);
- 20 e) an unblocking service for establishing a secure gateway and storing the UAC and UBC (Lipsit: page 5, lines 47-50; Chmaytelli: Col 8, lines 59-66);
- f) wherein the security device is configured to be accessed by a security device reader operatively connected and allowing access to a computer system to provide strong end user authentication (Lipsit: page 5, line 47 to page 6, line 17; Friedman: Col 16, lines 19-27);
- 25 Lipsit describes a system in which a secure gateway (38 of Fig 1) is used to coordinate unblocking of a security device. A subscription service provider transfers data into the secure gateway including serial numbers and security codes which assist in the unblocking process.

Lipsit, however, fails to disclose verification while an end user is in possession of the device. Specifically, it appears that the verification process for a user to receive a security code for a device takes place while a user is awaiting possession of a device (e.g. overnight delivery, second day delivery, etc) (page 5, lines 45-46) and not while the user is actually in possession of a device. Takae discloses the well-known idea that a verification process may take place while a user is in possession of a device. Combining the ideas of Takae with those of Lipsit allows the verification procedure to take place while the user is in possession of the device. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Takae with those of Lipsit makes the system more robust and secure for at least the reason that it provides more opportunity for authentication.

Lipsit in view of Takae disclose unblocking a remote device, but do not specifically disclose sending an unblock code to the device. In Lipsit in view of Takae, the unblocking of the device is done at the secure gateway.

Chmaytelli, discloses that a device may be physically locked and an unblock code may be sent to a device to unblock the device. Whereas Lipsit in view of Takae merely disclose unblocking of a device at a secure gateway, the combination as prescribed incorporates an unblock signal that may be received to further local unblocking of the device. Through the combination of Chmaytelli, the device in Lipsit in view of Takae's system may be physically blocked and requiring of an unblock code to be sent to locally render the device unblocked. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Chmaytelli with those of Lipsit in view of Takae because doing so makes the system more robust and secure because it incorporates the element that a device may be physically blocked and requiring of a local unblock code.

Lipsit in view of Takae in further view of Chmaytelli disclose limitations of the above claim. The combination further discloses that a security device (e.g. phone) may establish a connection with a security device reader (e.g. activation unit) in which parameters associated with the security device are read (Lipsit: page 6, lines 5-6) and communication and access is facilitated (Lipsit: page 6, lines 5-6 and 15-17). However, the combination appears to be silent as to utilization of *strong authentication*. Strong authentication is common and well-known in the art. For one example, Friedman teaches use of strong

Art Unit: 2137

authentication and further notes that strong authentication allows one to prove that it knows a secret without actually revealing the secret (Friedman: Col 16, lines 24-25). It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Friedman with those of Lipsit in view of Takae in further view of Chmaytelli because employing a strong authentication

5 technique makes a system more robust and secure.

As per claims 2 and 19, the applicant describes the apparatus of claims 1 and 18, which are met by Lipsit in view of Takae in further view of Chmaytelli in further view of Friedman, with the following limitation which is also met by Lipsit:

10       Wherein the security agent unblocks the security device from a remote location (page 5, line 47 to page 6, line 17).

As per claims 5 and 20, the applicant describes the apparatus of claims 1 and 18, which are met by Lipsit in view of Takae in further view of Chmaytelli in further view of Friedman, with the following

15 limitation which is also met by Lipsit:

Wherein the end user is remote (page 5, line 47 to page 6, line 17).

As per claim 7, the applicant describes the apparatus of claim 1, which is met by Lipsit in view of Takae in further view of Chmaytelli in further view of Friedman, with the following limitation which is also

20 met by Lipsit:

Wherein the apparatus is accessible via a web interface (page 5, lines 1-13).

As per claims 11-13 and 26, the applicant describes the apparatus of claims 1 and 18, which are met by Lipsit in view of Takae in further view of Chmaytelli in further view of Friedman, with the following

25 limitation which is met by Lipsit:

Wherein the UAC is accepted upon correlation of an end user identifier and a security device identifier (Lipsit: page 5, line 47 to page 6, line 17).

Art Unit: 2137

As per claims 29,36, and 37, the applicant describes a method of unblocking a security device issued to an end user using a security agent comprising the following limitations which are met by Lipsit, Takae, Chmaytelli, and Friedman:

- 5           a) gathering information from the end user and the security device (Lipsit: page 5, line 47 to page 6, line 17);
- b) verifying the information gathered from the end user and the security device (Lipsit: page 5, line 47 to page 6, line 17);
- c) contacting the security agent by the end user (Lipsit: page 5, lines 42-55);
- 10          d) supplying end user information verbally to the security agent (Lipsit: page 5, lines 42-55);
- e) verifying identity of the end user by the security agent using an identity verification mechanism (Lipsit: page 5, lines 42-55);
- f) generating an Unblock Authorization Code (UAC) after verification by the security agent, wherein verification comprises verifying the end user is assigned the security device while the end user is
- 15          in possession of the security device (Lipsit: page 5, line 47 to page 6, line 17; Takae: [0084]);
- g) delivering the UAC to an unblocking service (Lipsit: page 5, line 47 to page 6, line 17);
- h) storing the UAC against a security device record in a directory service (Lipsit: page 5, line 47 to page 6, line 17);
- i) supplying the UAC from the security agent to the end user (Lipsit: page 5, line 47 to page 6, line
- 20          17);
- j) applying the UAC to a client-side transfer agent by the end user (Lipsit: page 5, line 47 to page 6, line 17);
- k) delivering the UAC securely from the client-side transfer agent to the unblocking service (Lipsit: page 5, line 47 to page 6, line 17);
- 25          l) verifying the UAC of the client-side transfer agent and an agent-side transfer agent match through the unblocking service (Lipsit: page 5, line 47 to page 6, line 17);
- m) requesting an Unblock Code (UBC) from the directory service (Chmaytelli: Col 8, lines 59-63);

Art Unit: 2137

o) unblocking the security device by transferring the UBC from the directory service to the client-side transfer agent (Chmaytelli: Col 8, lines 59-63);

p) wherein the unblocking service stores the UAC and the UBC (Lipsit: page 5, line 47 to page 6, line 17; Chmaytelli: Col 8; lines 59-63);

5           q) wherein the security device is configured to be accessed by a security device reader operatively connected and allowing access to a computer system to provide strong end user authentication (Lipsit: page 5, line 47 to page 6, line 17; Friedman: Col 16, lines 19-27);

Motivation for combination is substantially the same as that provided in the rejection of claim 1.

10           As per claims 30-32, the applicant describes the method of claim 29, which is met by Lipsit in view of Takae in further view of Chmaytelli in further view of Friedman, with the following limitation which is met by Lipsit:

Wherein the security device identifier is a serial number (Lipsit: page 5, line 47 to page 6, line 17).

15           Claims 3-4 and 22-23 rejected under 35 U.S.C. 103(a) as being unpatentable over Lipsit in view of Takae in further view of Chmaytelli in further view of Friedman in further view of Menezes, (Menezes, Alfred J. Handbook of Applied Cryptography. 1997. CRC Press. Pages 15-17 and 388-390).

20           As per claims 3 and 22, the applicant describes the apparatus of claims 1 and 18, which are met by Lipsit in view of Takae in further view of Chmaytelli in further view of Friedman, with the following limitation which is met by Menezes:

Wherein an end user identifier and a password is presented by the end user for the client-side transfer agent to connect to the unblocking service (Menezes: 388);

25           Lipsit in view of Takae in further view of Chmayelli in further view of Friedman discloses all the limitations of claims 1 and 18. The combination also discloses that a password may be presented by the end user for the client-side transfer agent to connect to the unblocking service (page 4, lines 51-54). The



Art Unit: 2137

combination, however, does not disclose that the password is presented with an end user identifier as an end user/password pair.

Menezes discloses the idea that a password is typically presented with an end user identifier as an end user identifier/password pair. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Menezes with those of Lipsit in view of Takae in further view of Chmaytelli in further view of Friedman because authenticating an end user with an end user identifier/password pair allows each end user to maintain their own personal password rather than just having one universal password. This enhances security in the system because a hacker needs to know two pieces of information (the end user identifier and the password) instead of just one piece of information.

As per claims 4 and 23, the applicant describes the apparatus of claims 1 and 18, which are met by Lipsit in view of Takae in further view of Chmaytelli in further view of Friedman, with the following limitation which is met by Menezes:

Wherein the secure gateway is configured to perform an authentication process for every transfer between the client-side transfer agent and the unblocking service (Menezes: 15).

Lipsit in view of Takae in further view of Chmaytelli in further view of Friedman appears to be silent as to how data is transferred between the client-side transfer agent and the unblocking service. If the data were encrypted with a symmetric key, an authentication process would be performed for every data transfer since only an authorized user should have the symmetric key.

Claims 10 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lipsit in view of Takae in further view of Chmaytelli in further view of Friedman in further view of Binder, U.S. Patent Application Publication No. 2002/0138553.

Art Unit: 2137

As per claims 10 and 25, the applicant describes the apparatus of claims 1 and 18, which are met by Lipsit in view of Takae in further view of Chmaytelli in further view of Friedman, with the following limitation which is met by Binder:

5 The client-side transfer agent is configured to check periodically at a configurable frequency for the UAC (Binder: [0036]);

Lipsit in view of Takae in further view of Chmaytelli in further view of Friedman disclose all the limitations of claims 1 and 18. However, the combination does not disclose checking at a configurable frequency for the UAC.

10 Binder discloses this idea in a networking system in which a client is set to check at a configurable frequency for a generated message. As disclosed by Binder, this functionality is advantageous because it eliminates the costly and unnecessary need for the user to maintain a constant open connection between a client and a server [0027]. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Binder with those of Lipsit in view of Takae in further view of Chmaytelli in further view of Friedman because having a client check for a UAC  
15 at a configurable frequency eliminates the costly and unnecessary need for the user to maintain a constant open connection with the unblocking service.

Claim 28 is rejected under 35 U.S.C. 103(a) as being unpatentable over Lipsit in view of Menezes in further view of Takae in further view of Chmaytelli in further view of Binder in further view of Friedman.

20

As per claim 28, the applicant describes a method of unblocking a security device issued to an end user comprising the following limitations which are met by Lipsit, Menezes, Takae, Chmaytelli, Binder, and Friedman:

25 a) establishing a secure gateway by an unblocking service (Lipsit: Fig 1; page 5, line 47 to page 6, line 17);

b) transferring information among the unblocking service, the end user, and the security device in a secure manner (Lipsit: page 5, line 47 to page 6, line 17);

Art Unit: 2137

c) transferring information between the unblocking service and the security agent in a secure manner (Lipsit: page 5, line 47 to page 6, line 17);

d) presenting an end user identifier and a password pair by the end user for a client-side transfer agent (Lipsit: page 4, lines 51-54; Menezes: page 388);

5 e) performing an authentication process for every transfer between the client-side transfer agent and the unblocking service (Lipsit: page 4, lines 51-54; Menezes: page 15);

f) generating an Unblock Authorization Code (UAC) after verification by a security agent, wherein verification comprises verifying the end user is assigned the security device while the end user is in possession of the security device (Lipsit: page 5, lines 47-50; Takae: [0084]);

10 g) transferring the UAC securely from an agent-side transfer agent to the unblocking service (Lipsit: page 5, line 47 to page 6, line 17);

g) supplying the UAC to the end user by the security agent (Lipsit: page 5, line 47 to page 6, line 17);

15 h) applying the UAC to the client-side transfer agent by the end user (Lipsit: page 5, line 47 to page 6, line 17);

i) transferring the UAC securely from the client-side transfer agent to the unblocking service (Lipsit: page 5, line 47 to page 6, line 17);

j) verifying the UAC transferred by the client-side transfer agent and the agent-side transfer agent match through the unblocking service (Lipsit: page 5, line 47 to page 6, line 17);

20 k) transferring an Unblock Code (UBC) securely from the unblocking service to the client-side transfer agent (Chmaytelli: Col 8, lines 59-66);

l) unblocking the security device using the UBC (Chmaytelli: Col 8, lines 59-63);

m) checking at a configurable frequency to determine whether the UAC is generated (Binder: [0036]);

25 n) correlating the end user identifier and a security device identifier prior to acceptance of the UAC (Lipsit: page 5, line 47 to page 6, line 17);

Art Unit: 2137

o) providing the UBC by the unblocking service to the client-side transfer agent after correlation of the end user identifier, the password pair, and the security device identifier (Chmaytelli: Col 8, lines 59-63).

p) wherein the unblocking service stores the UAC and the UBC (Chmaytelli: Col 8, lines 59-63; Lipsit: page 5, line 47 to page 6, line 17);

q) wherein the security device is configured to be accessed by a security device reader operatively connected and allowing access to a computer system to provide strong end user authentication (Lipsit: page 5, line 47 to page 6, line 17; Friedman: Col 16, lines 19-27).

10 Claims 8, 14-16 and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lipsit in view of Takae in further view of Chmaytelli in further view of Friedman in further view of Menezes.

As per claims 14-16, and 27, the applicant describes the apparatus of claims 1 and 18, which are met by Lipsit in view of Takae in further view of Chmaytelli in further view of Friedman, with the following  
15 limitation which is met by Menezes:

Wherein the UBC is provided by the unblocking service to the client-side transfer agent after correlation of an end user identifier, a password pair, and a security device identifier (Menezes: page 388);

Lipsit in view of Takae in further view of Chmaytelli in further view of Friedman discloses all the  
20 limitations of claims 1 and 18. Lipsit also discloses that a password may be presented by the end user for the client-side transfer agent to connect to the unblocking service (page 4, lines 51-54). The combination, however, does not disclose that the password is presented with an end user identifier as an end user/password pair.

Menezes discloses the idea that a password is typically presented with an end user identifier as  
25 an end user identifier/password pair. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Menezes with those of Lipsit in view of Takae in further view of Chmaytelli in further view of Friedman because authenticating an end user with an end

Art Unit: 2137

user identifier/password pair allows each end user to maintain their own personal password rather than just having one universal password. This enhances security in the system because a hacker needs to know two pieces of information (the end user identifier and the password) instead of just one piece of information.

5

As per claim 8, the applicant describes the apparatus of claim 3, which is met by Lipsit in view of Takae in further view of Chmaytelli in further view of Friedman in further view of Menezes, with the following limitation which is met by Chmaytelli:

Wherein the end user identifier is an e-mail address (Chmaytelli: Col 8, lines 54-59).

10

Claim 33 is rejected under 35 U.S.C. 103(a) as being unpatentable over Lipsit in view of Takae in further view of Chmaytelli in further view of Friedman in further view of Rosenberg, U.S. Patent Application Publication No. 2003/0013434.

15

As per claim 33, the applicant describes the method of claim 29, which is met by Lipsit in view of Takae in further view of Chmaytelli in further view of Friedman, with the following limitations which are met by Chimaytelli and Rosenberg:

- a) generating a new UBC (Chimaytelli: Col 8, lines 59-63; Rosenberg: [0072] to [0075]);
- b) setting the security device to the new UBC (Rosenberg: [0072] to [0075]);
- c) delivering the new UBC to the directory service (Rosenberg: [0072] to [0075]);

20

Lipsit in view of Takae in further view of Chmaytelli in further view of Friedman disclose all the limitations of claim 29. Chmaytelli also discloses the idea of retrieving a UBC and sending the UBC to a security device so that it can be applied to unblock the device. Chmaytelli does not disclose the idea of generating a new UBC: Chmaytelli is silent as to whether the UBC is generated or simply retrieved from a list of existing UBCs.

25

Rosenberg discloses the idea of generating a UBC (activation code) for a user and delivering the new UBC to a directory service where it can be obtained by a user. It would have been obvious to one of

Art Unit: 2137

ordinary skill in the art at the time the invention was filed to combine the ideas of Rosenberg with those of Lipsit in view of Takae in further view of Chmaytelli in further view of Friedman because generating a UBC instead of just retrieving it from a list enhances security in the system by generating fresh activation codes thereby curtailing the amount of time a hacker has to steal the activation code.

5

Claim 34 is rejected under 35 U.S.C. 103(a) as being unpatentable over Lipsit in view of Takae in further view of Chmaytelli in further view of Friedman in further view of Angelo, U.S. Patent No. 5,949,882.

10 As per claim 34, the applicant describes the method of claim 29, which is met by Lipsit in view of Takae in further view of Chmaytelli in further view of Friedman, with the following limitation which is met by Angelo:

Verifying the security device is not already permanently blocked (Angelo: Col 11, lines 8-16);

15 Lipsit in view of Takae in further view of Chmaytelli in further view of Friedman disclose all the limitations of claim 29. However, the combination does not disclose verifying that the security device is not already permanently blocked. Angelo discloses a system in which a check is made on a security device to make sure it is not permanently blocked. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Angelo with those of Lipsit in view Takae in further view of Chmaytelli in further view of Friedman because checking to make sure a device is  
20 not permanently blocked makes the system more efficient because resources are not wasted trying to unblock a device which is permanently blocked.

Claim 35 is rejected under 35 U.S.C. 103(a) as being unpatentable over Lipsit in view of Takae in further view of Chmaytelli in further view of Rosenberg in further view of Angelo in further view of  
25 Friedman.

Art Unit: 2137

As per claim 35, the applicant describes a method of unblocking a security device issued to an end user comprising the following limitations which are met by Lipsit, Takae, Chmaytelli, Rosenberg, Angelo, and Friedman:

- 5 a) gathering information from the end user and the security device (Lipsit: page 5, line 47 to page 6, line 17);
- b) verifying the information gathered from the end user and the security device (Lipsit: page 5, line 47 to page 6, line 17);
- c) contacting the security agent by the end user (Lipsit: page 5, line 47 to page 6, line 17);
- d) supplying end user information to the security agent (Lipsit: page 5, line 47 to page 6, line 17);
- 10 e) verifying identity of the end user by the security agent using an identity verification mechanism (Lipsit: page 4, lines 51-54);
- f) generating an Unblock Authorization Code (UAC) after verification by the security agent, wherein verification comprises verifying the end user is assigned the security device while the end user is in possession of the security device (Lipsit: page 5, line 47 to page 6, line 17; Takae: [0084]);
- 15 g) transferring the UAC to an unblocking service (Lipsit: page 5, line 47 to page 6, line 17);
- h) storing the UAC against a security device record in a directory service (Lipsit: page 5, line 47 to page 6, line 17);
- i) transferring the UAC to an unblocking service (Lipsit: page 5, line 47 to page 6, line 17);
- j) storing the UAC against a security device record in a directory service (Lipsit: page 5, line 47 to 20 page 6, line 17);
- k) supplying the UAC from the security agent to the end user (Lipsit: page 5, line 47 to page 6, line 17);
- l) applying the UAC to a client-side transfer agent by the end user (Lipsit: page 5, line 47 to page 6, line 17);
- 25 m) delivering the UAC securely from the client-side transfer agent to the unblocking service (Lipsit: page 5, line 47 to page 6, line 17);

Art Unit: 2137

n) verifying the UAC transferred by the client-side transfer agent and an agent-side transfer agent match through the unblocking service (Lipsit: page 5, line 47 to page 6, line 17);

o) requesting an Unblock Code (UBC) from the directory service (Chmaytelli: Col 8, lines 59-66);

p) unblocking the security device by transferring the UBC from the directory service to the client-side transfer agent (Chmaytelli: Col 8, lines 59-66);

q) gathering information from the end user using the client-side transfer agent (Lipsit: page 5, line 47 to page 6, line 17);

r) gathering information from the security device using the client-side transfer agent (Lipsit: page 5, line 47 to page 6, line 17);

s) generating a new UBC (Rosenberg: [0072] to [0075]);

t) setting the security device to the new UBC (Rosenberg: [0072] to [0075]);

u) delivering the new UBC to the directory service (Rosenberg: [0072] to [0075]);

v) verifying the security device is not already permanently blocked (Angelo: Col 11, lines 8-16),

w) wherein the unblocking service stores the UAC and the UBC (Rosenberg: [0072] to [0075]);

x) wherein the security device is configured to be accessed by a security device reader operatively connected and allowing access to a computer system to provide strong end user authentication (Lipsit: page 5, line 47 to page 6, line 17; Friedman: Col 16, lines 19-27).

### ***Response to Arguments***

Applicant's Information Disclosure Statement (IDS) filed December 8, 2003 has been considered and placed in the file.

Applicant's arguments, see Remarks, filed 6/29/06, with respect to the 103(a) rejection(s) of claim(s) 1-8, 10-16, 18-23, and 25-37 under various prior art references have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made with regard to all pending claims except claims 6 and 21.



Art Unit: 2137

**Conclusion**

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

5 A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of  
10 the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kevin Schubert whose telephone number is (571) 272-4239. The examiner can normally be reached on M-F 7:30-6:00.

15 If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from  
20 either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-  
25 1000.

KS

*Jacques Louis-Jacques*  
JACQUES LOUIS-JACQUES  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100